Figure 1

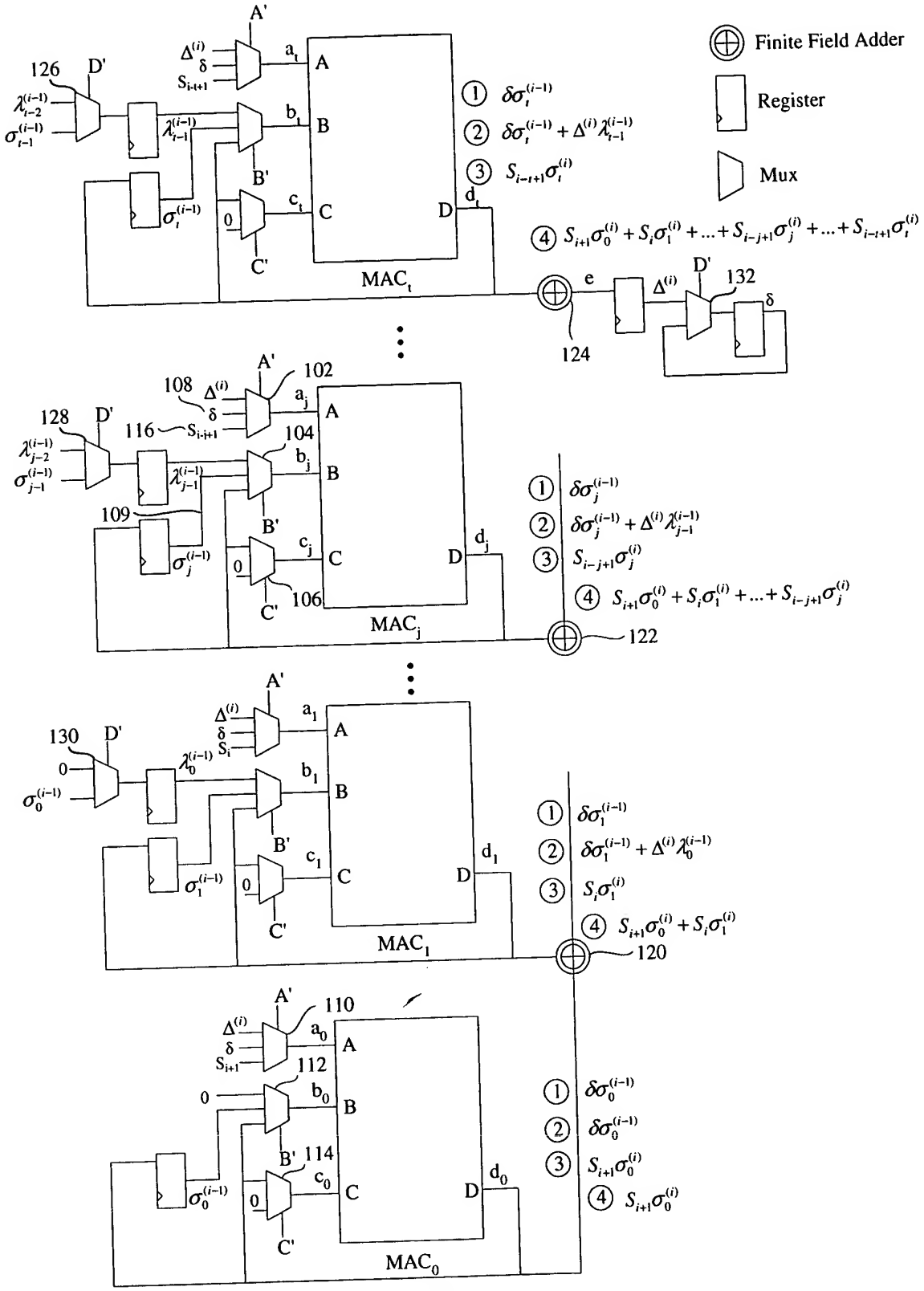
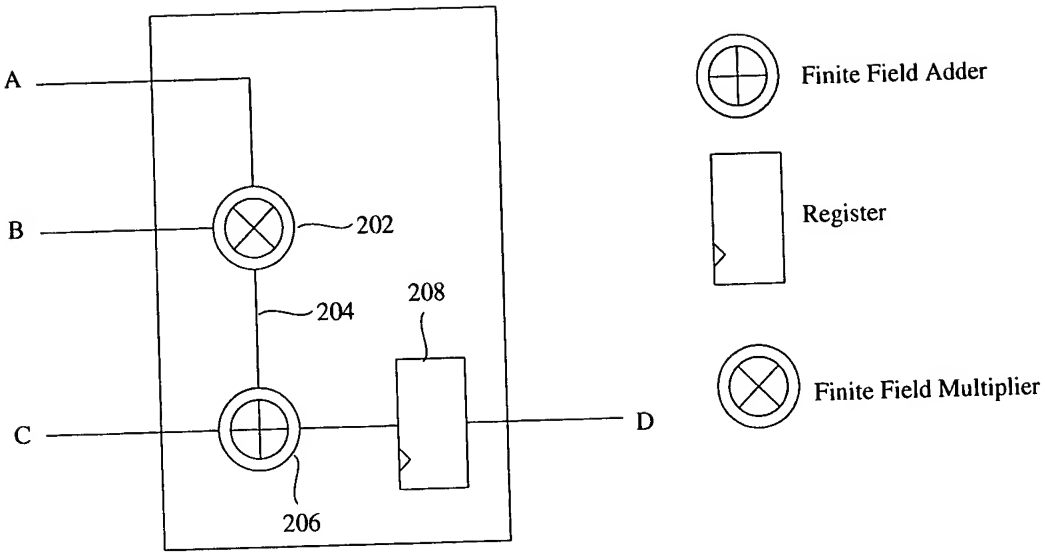
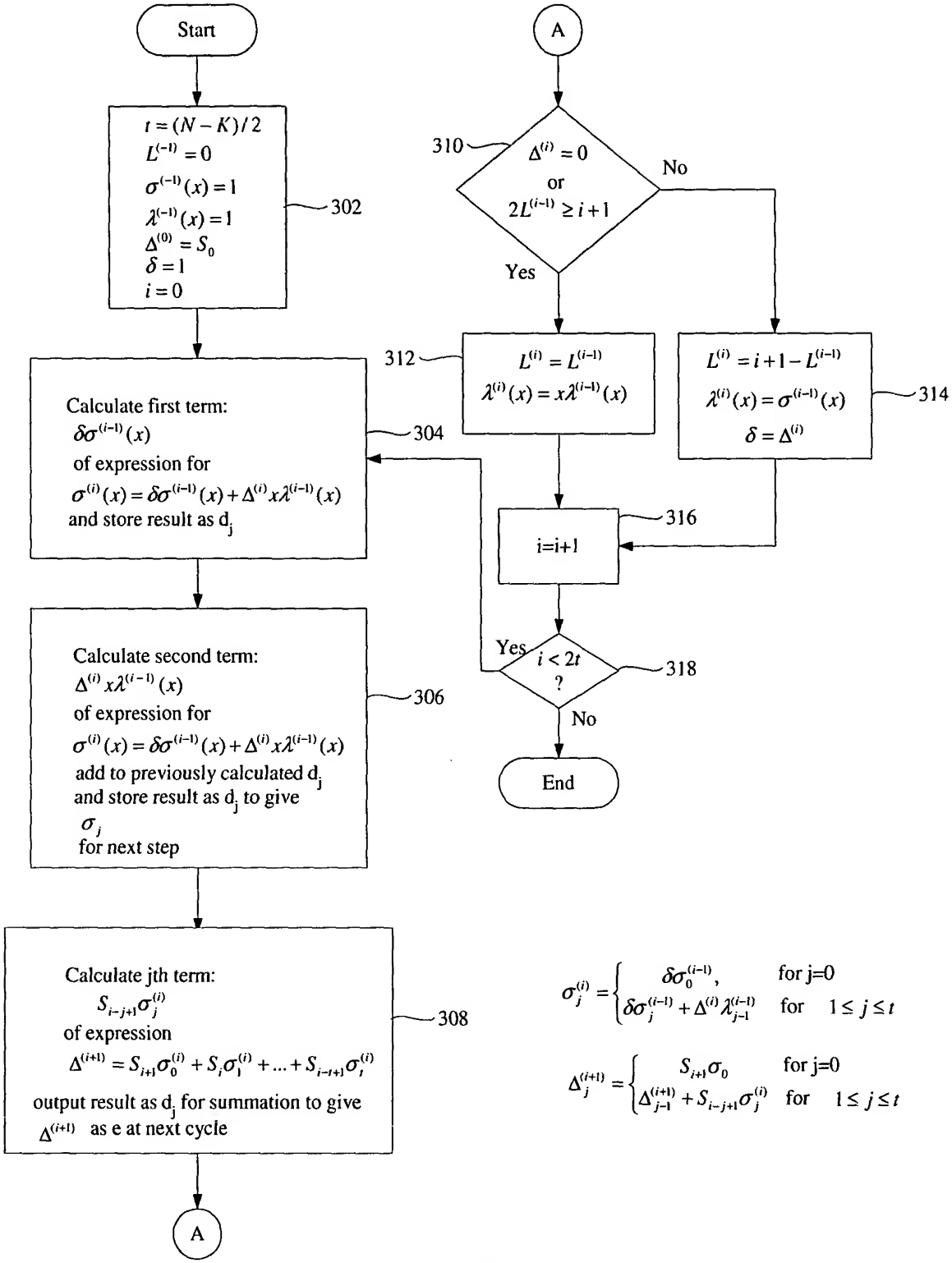

Finite Field Adder
Register
Mux
MAC_t
MAC_j
MAC_1
MAC_0
100
120
122
124
126
128
130
102
104
106
108
109
110
112
114
116
132

Figure 2


A
B
C
D
202
204
206
208
Finite Field Adder
Register
Finite Field Multiplier

200

Figure 3



$$\sigma_j^{(i)}=\begin{cases}\delta\sigma_0^{(i-1)}, & \text{for j=0}\\ \delta\sigma_j^{(i-1)}+\Delta^{(i)}\lambda_{j-1}^{(i-1)} & \text{for } 1\leq j\leq t\end{cases}$$

$$\Delta_j^{(i+1)}=\begin{cases}S_{i+1}\sigma_0 & \text{for j=0}\\ \Delta_{j-1}^{(i+1)}+S_{i-j+1}\sigma_j^{(i)} & \text{for } 1\leq j\leq t\end{cases}$$

Figure 4

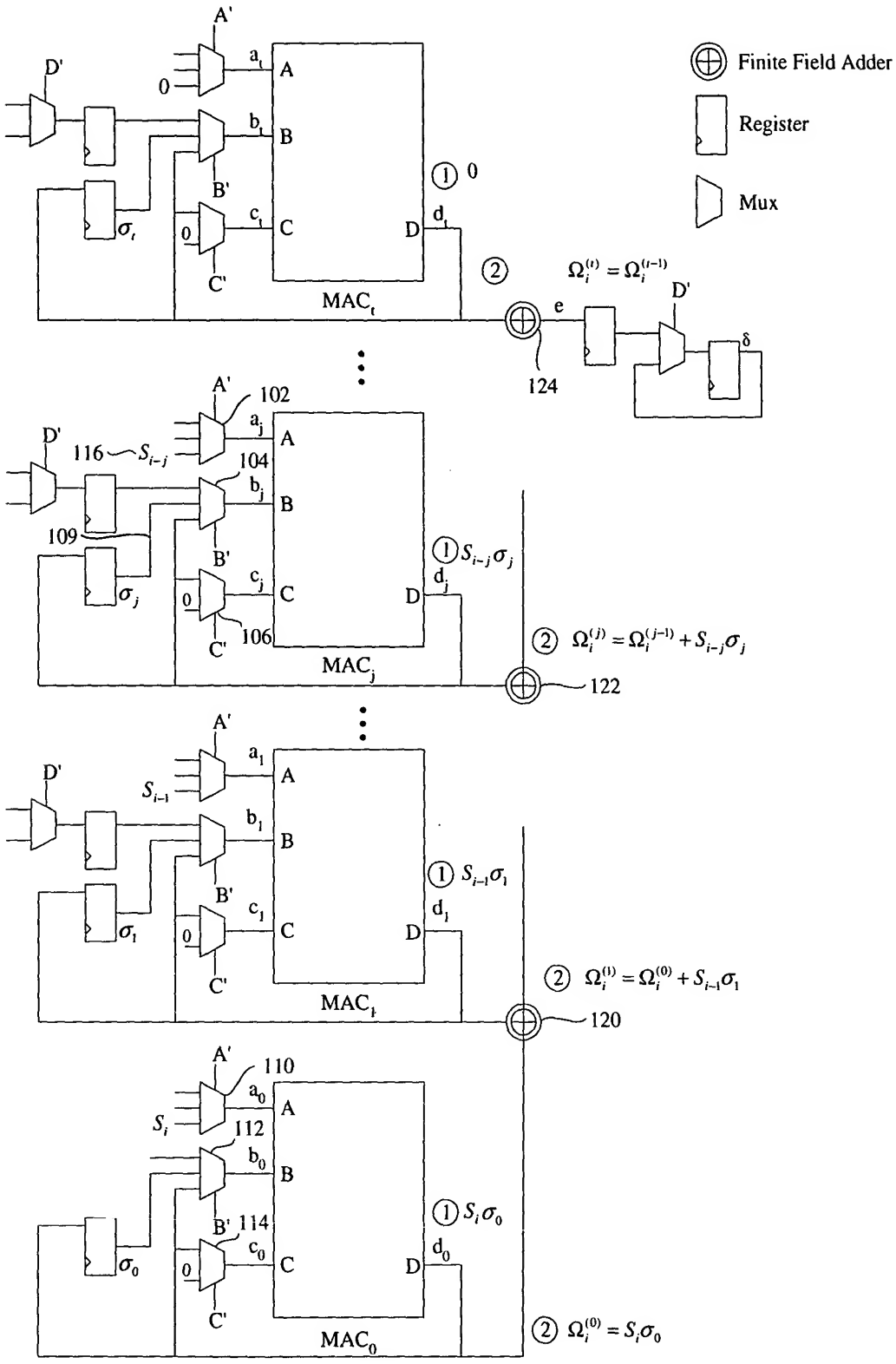
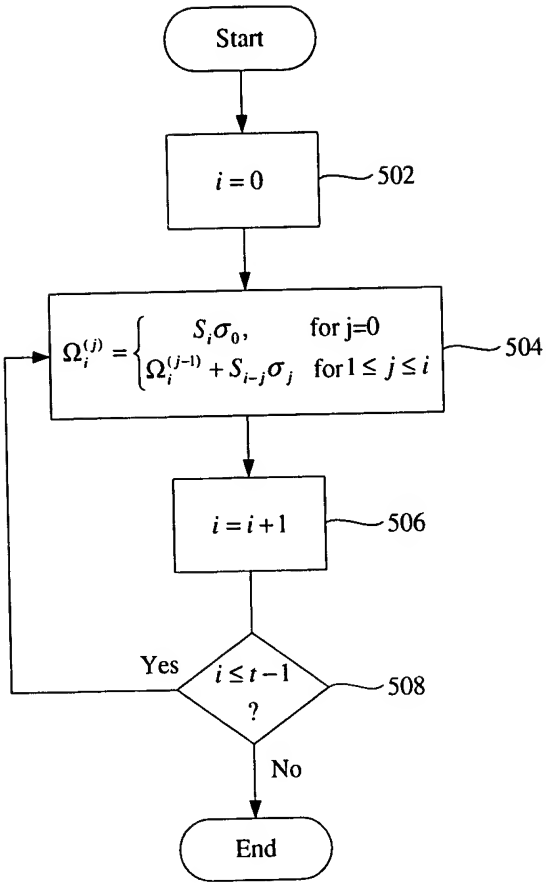

Finite Field Adder
Register
Mux
A'
D'
0
a_t
A
b
B
B'
c_t
C
C'
D
d_t
σ_t
MAC_t
① 0
② $\Omega_i^{(t)} = \Omega_i^{(t-1)}$
e
124
D'
δ
102
a_j
116 S_{i-j}
104
b_j
109
σ_j
c_j
106
d_j
MAC_j
① $S_{i-j}\sigma_j$
② $\Omega_i^{(j)} = \Omega_i^{(j-1)} + S_{i-j}\sigma_j$
122
a_1
S_{i-1}
b_1
c_1
d_1
σ_1
MAC_1
① $S_{i-1}\sigma_1$
② $\Omega_i^{(1)} = \Omega_i^{(0)} + S_{i-1}\sigma_1$
120
110
a_0
S_i
112
b_0
114
c_0
d_0
σ_0
MAC_0
① $S_i\sigma_0$
② $\Omega_i^{(0)} = S_i\sigma_0$
400

Figure 5


Start
$i = 0$
502
$\Omega_i^{(j)} = \begin{cases} S_i\sigma_0, & \text{for j=0} \\ \Omega_i^{(j-1)} + S_{i-j}\sigma_j & \text{for } 1 \le j \le i \end{cases}$
504
$i = i + 1$
506
Yes
$i \le t-1$
?
508
No
End